Cryptology ePrint Archive: Report 2011/044

Fast Scalar Multiplication in ECC using The Multi base Number System.

G. N. Purohit , Asmita Singh Rawat

Abstract: As a generalization of double base chains, multibase number system is very suitable for efficient computation of scalar multiplication of a point of elliptic curve because of shorter representation length and hamming weight. In this paper combined with the given formulas for computing the 7- Fold of an elliptic curve point P an efficient scalar multiplication algorithm of elliptic curve is proposed using 2,3 and 7 as basis of the multi based number system . The algorithms cost less compared with Shamirs trick and interleaving with NAFs method.

Category / Keywords: applications / elliptic curve cryptosystem

Date: received 22 Jan 2011

Contact author: singh asmita27 at gmail com